Digitalization of port access control: case study Port of Šibenik

S. Aksentijević*, E. Tijan**, A. Panjako*** and G. Mrčela****
* Aksentijević Forensics and Consulting, Ltd, Viškovo, Croatia
sasa.aksentijevic@gmail.com
** University of Rijeka, Faculty of Maritime Studies/Department of logistics and management, Rijeka, Croatia
etijan@pfri.hr
*** Ca' Foscari University of Venice, Department of management, Venice, Italy
ana.panjako95@gmail.com
**** Port of Šibenik Authority, Šibenik, Croatia
info@portauthority-sibenik.hr

Abstract **- The aim of this paper is to research and describe the legacy situation in the Port of Šibenik related to port access procedures and control, as they are identified within the scope of 2014 - 2020 Interreg V-A Italy - Croatia project "Digitalising Logistics processes – DigLogs". Furthermore, main findings and opportunities for optimization are identified and presented along with a carefully selected integral business information management solution that will be developed as a part of the pilot project in order to streamline access control procedures, and increase port security and target group stakeholder' satisfaction.**

Keywords – port security; access control; Port of Šibenik; DigLogs project; pilot solution

I. INTRODUCTION

In the EU, the attention to improvement of the quality, safety and environmental sustainability of marine and coastal transport services and nodes by promoting multimodality is one of the specific objectives to be promoted through financed projects [1]. An Interreg 2014 - 2020 V-A Italy – Croatia project "Digitalising Logistics processes -– DigLogs" aims to create the necessary concepts, technological solutions, models and plans to establish the most advanced digitalized logistic processes for multimodal freight transport and passengers' services in the Programme Area. The project objectives are linked to the digitalisation of transport services. There are several types of barriers hindering the proliferation of multimodality and a clear harmonisation of passenger services both in Italy and in Croatia, including organizational barriers (e.g. lack of transparency, unclear responsibility in the transport chain), technical barriers (e.g. friction at transfer points, lack of standardization of equipment and loading units, missing information flows), financial and economic barriers (perceived high costs of investment in intermodal infrastructure), and infrastructure barriers.

Port of Šibenik Authority is the institution that manages the port of Šibenik. Apart from the cargo port, it is lately one of the most heavily utilized Adriatic passenger and cruise ports [2]. Port of Šibenik Authority is founded to govern, construct and use the Port of Šibenik, opened for international public transport, and proclaimed as the port of special international and economic interest for the Republic of Croatia. The Port Authority assigns concessions for port activities based on valid technical and technological conditions, after the public tendering.

Port of Šibenik Authority seized the opportunity of DigLogs cooperation to funnel knowledge and acquired financing to further foster the development of IT systems in order to support the digitalization, by incorporating the structural access control and ensuring port security according to applicable set of regulations. As a result, and within scope of a DigLogs projects, it has executed a pilot project aimed to digitalise these processes [3].

II. PILOT PROJECT PURPOSE AND GOALS

The project goal is to establish a new, innovative and automatic solution for passenger and physical persons ID card issuing, tracking and management within the remit of Port of Šibenik Authority, with particular focus on the passenger traffic. This need is greatly increased with the fact that creation of a national Port Community System (PCS) is ongoing, and it does not have a dedicated system for access control.

PCS needs to be connected to the surrounding systems with an underlying goal being the avoidance of multiple data entry and the facilitation of data exchange between stakeholders. The "Project of setting up a single national Port Community System" is currently underway, with the Ministry of the Sea, Transport and Infrastructure being the bearer of the project. Cooperating parties in this project are, among others, Port of Rijeka Authority and Port of Ploče Authority [4]. Once the mentioned project is completed, all the Croatian port authorities will have access to a fully functional PCS system that will be adjusted to participating ports (including the Port of Šibenik) after individual adjustments and adaptation dependent on local characteristics.

The layout of operative quays of the port of Šibenik is shown in the map below (Fig. 1).

Figure 1: Port of Šibenik operative quays

It is immediately apparent that the port has quite a diverse structure and many quays serving different purposes and having their distinct characteristics. Quays designations, names, length, depth and purposes are shown in Table 1.

Each PCS is specific, each country has individual legal regulations and therefore each port community develops its own PCS according to its needs [5]. A decision on the pilot content was made because it immediately came to the attention of the Port of Šibenik Authority's management that there is room for the implementation of an innovation within scope of the DigLogs project.

In its essence, the port access control solution is a sustaining incremental innovation that digitalizes a process that is currently executed manually and presents a large obstacle in modernization of processes inside port of Šibenik, but is also not addressed within the scope of the new to-be PCS system that will eventually be deployed in the port of Šibenik.

TABLE I. OPERATIVE CHARACTERISTICS OF PORT OF ŠIBENIK'S QUAYS

Designation	Name	Length (m)	Depth (m)	Purpose
8-9	Vrulje, W1	114	10,00	Ferryboats
10	Vrulje, W2	50	10,00	Ferryboats
11	Vrulje, S1	133	08,00	Cruise lines
12	Vrulje, S2	29	10,00	Customs
13	Vrulje, E	191	10,00	Cruise lines
Cargo port				
14	Dobrika	228	10,00	Bulk cargo import
15	Connection coast	128	08,00	RO RO, Ferryboats
16	Rogač 1	210	10,00	Bulk and general cargo
17	Rogač 2	240	07,00 - 09,00	Bulk and general cargo
19	TB 1	120	07,00	Timber terminal
20	TB 1	120	05,20	Timber terminal

Considering the required synergies between public and private stakeholders in order to improve the efficiency and competitive positions of the seaport communities [6], decision has been made to implement a new *digital access control system, fully aligned with current business needs, whose full scope is to be defined within the pilot work plan*, encompassing stakeholders whose activities are aimed towards the processes underlying passengers disembarking and boarding cruisers and passenger ships, port concessionaires, business personnel, vehicles, drivers, containers and other stakeholders within identified target groups. Presently, access control to the Port of Šibenik area is governed by the "Regulation about identification cards" of the Port of Šibenik Authority from 2015. ID cards used for ingress and egress control and access to information, cargo, premises and operative port spaces are used to identify persons and vehicles and they are particular to a certain person or vehicle and non-transferrable. There is also a quite detailed pricing list for permit issuing, as it presents a source of revenue for the Port of Šibenik Authority, in force as of 6th January 2017.

The envisaged pilot project already contains the integration with more complex solutions and provides insight to external involved parties (police – Ministry of the interior) and in the future can interface with internal business information system used by the Port of Šibenik Authority and the national Maritime Single Window solution, CIMIS [7].

III. PILOT PROJECT FUNCTIONS, SCOPE AND METHODOLOGY

The Purpose of this pilot project is the enhancement of security and safety in the port area including payment, tracking, oversight and analysis solutions. It should serve as an input solution for further connection with the national PCS system, whose implementation is ongoing in parallel with this pilot project.

The pilot scope is represented by the requisitioning and purchase of the envisaged equipment, its installation and functional integration, development of the web and mobile applications aimed towards administration, passengers and the police, and the implementation of analytic capabilities for the system.

The exact technical requirements, connectivity and input-output possibilities are subject to further refining during pilot development and component identification up to its end, as some components might change even during the pilot execution. While main components were already identified as a part of analysis and requirements specification, some smaller components have to be identified later in the pilot execution, so flexibility is required during subsequent execution stages.

The existing access control processes are still implemented in physical form, using manual labour and plastic cards, causing delays, excessive consumption of time and other resources, and diminishing integration and analytics, contrary to the International Ship and Port Facility Security Code (ISPS) requirements and modern business process execution inside ports. This is especially prevalent when processing large number of passengers

from cruisers whose access permits need to be manually processed, sometimes even overnight. For example, passenger terminal Vrulje with a cumulative quay length of 510 meters, has a projected capacity of 1.000.000 passengers annually and with the ongoing capacity expansion to 2.000.000 passengers annually, an inherent need for a new digital system of permits issuing based on innovative digital solution is even more clear.

A required innovative passenger ID card issuing, and control system must possess adequate technical qualities to support the envisaged role. Also, a compliance with the existing regulations already used in Port of Šibenik was a must-have requirement for the pilot.

Pilot project limitations are primarily in form of focus on only passenger area, omitting other port areas (for example, areas processing maritime cargo). Port of Šibenik has a quite diverse port structure, and full coverage would have greatly exceeded the budget and the scope of the proposed pilot project.

Project assumptions are:

1. Time frame dedicated for pilot execution will be adequate,
2. Financial means for pilot requisitioning will suffice,
3. There are suitable locations for uninterrupted installation and operative usage of the ID card reading equipment,
4. The stakeholders will be interested in the project deliverables and satisfied with the project outcomes,
5. Port access and ID issuing regulations might have to be revised as a consequence of the pilot execution.

Custom project management methodology will be used, based on PMI-PMP methodology, covering the entire lifecycle of the pilot project implementation. It is best suited to the fast track and relatively short projects like this pilot, with approximate duration of 9 months.

Expected output documents produced as a part of the pilot project are:

1. Pilot Work Plan (project charter),
2. Functional – technical pilot specification (serves as a basis for tendering documentation),
3. Tendering documentation (used in the public procurement process),
4. Installation and development logs and related documentation,
5. Equipment delivery and integration (development) services delivery notes,
6. User manuals and additional documentation,
7. Invoicing documentation,
8. Communication archives (emails).

Monitoring of the pilot project execution will be executed using the following milestones, in sequence (check points):

1. Compiled draft of the project work plan – approved by the Port of Šibenik Authority,
2. Completed project work plan, ← CHECK OFF MILESTONE 1
3. Written draft of the technical-functional specification,
4. Completed rest of the public procurement (tendering) documentation,
5. Issued requests/invitations for quotations,
6. Received commercial offers,
7. Evaluation of offers completed and best offers selected,
8. Awarded integration and development services contracts, ← CHECK OFF MILESTONE 2
9. Equipment delivered and installed,
10. Integration development services delivered and completed,
11. User Acceptance Testing (UAT), and
12. Full system functional (pilot development completed). ← CHECK OFF MILESTONE 3

IV. CURRENT STATE-OF-THE-ART, PROJECT PREPARATION AND SOLUTION DESIGN

At the moment, according to the applicable regulations [8, 9], there are two levels of used ID cards, and articles 8-14 of the applicable regulation govern layout, characteristics and use of ID cards.

Physical cards can be divided into the following categories:

1. *Red colour cards*
   - Employees of Port of Šibenik Authority,
   - Internal security personnel,
   - External security personnel (vigilance), and
   - State employees (police officers, Customs officers, employees of Harbourmaster's office, employees of the State inspectorate).
2. *Blue colour cards*
   - Concessionaires using port infrastructure and superstructure,
   - Concessionaires not using port infrastructure and superstructure,
   - Ship agents with work permits,
   - Shipping agencies in the area of port of Šibenik,
   - Cargo agents, and

- Subcontractors of the concessionaires.

3. *Light grey colour cards* – temporary vendors and contractors
4. *Green colour cards*
   - Visitors, and
   - Commercial activity parties (recording of marketing materials, documentaries or TV shows).

The process is not presently digitalized and there is no connection whatsoever with other IT systems. Issuing and tracking relies on manual procedures. Also, no systematic analysis is possible, including statistics, cross-referencing and data import or export for categories of users other than those accessing port areas using cargo vehicles. This lack of complete informatization of access control process can be identified as an evident bottleneck, especially in relation to ISPS requirements and port security procedures.

Entry and exit terminals to and from the port are to be designated as positions where the ID cards are checked, in order to allow entry and exit. Initially and within the pilot scope, they include locations (entry to quays and terminals) that are mostly affected by the flow of the passenger traffic.

The analysis has shown that the deployment of a modern, innovative digital access control and preparation for full integration of access control system with the future PCS is critical at the moment of pilot action analysis and proposal, especially considering the lack of funding, and no funds anticipated at the PCS side to cover the aforementioned functionalities (mainly the access control).

Affected stakeholders within the identified targeted groups (apart from passengers) are all cargo agents operating in port of Šibenik, all inland cargo traffic operators (categorized for simplicity as one entity) and all other occasional or permanent visitors to the port area (police, Customs officers, other state agency officials, vendors, consultants, subcontractors, teams filming in the port area etc.) who need to fill paper documents in order to obtain access to port area [10]. In the current scope of the national PCS, no module is envisaged to support the permit issuing due to time and financial constraints.

It is evident that in order to increase digitization in the area of port of Šibenik for almost all stakeholders (especially passengers), further steps need to be undertaken in order to upgrade processes and technology by introducing and building a completely new innovative IT system to facilitate permit issuance, storage, monitoring and oversight, further underlining ISPS compliance [11]. The permits will therefore become digital products whose status can be checked from any physical place by using tools embedded in the system. In order to automatize the system, every access permit will have a unique identification code (for example, a QR code) that will be embedded and enable cross-checking with other data from the permit. Content of the QR code is hash string derived using ID-number encrypting by SHA-x methodology. Full digitalization should ensure traceability and follow up to every request for permit issuing. Digitalization will enable additional functions for better traffic management and tracing port resources and increase general level of security. End users will gain higher service levels and lowered levels of stress, as they will be able to perform all these actions in advance and remotely.

The basic characteristic of the system is on-line work. It includes dislocated, centralized and unique database with remote access in real time. A database is the only location for data storage and interexchange in the system.

Communication with the database is achieved using web services that are a part of a broader application layer: local applications, portable applications and the Web communication with the database using only web services. Basic architecture of the application is shown in the Fig. 2.

This type of solution (scalable cloud) enables good overview of the system operations, protects data and raises level of system availability. It ensures the required SLA (Service Level Agreement) levels. This solution requires a quality local IT infrastructure (LAN and web access with low latency levels).

The system includes the following elements:

1. *E-mail and SMS notification* subsystems following the highest industry standards and guaranteeing user reach inland and abroad,
2. *Payment gateway* for credit card payment on the web for domestic and foreign users,
3. *Interface* towards *ingress and egress equipment* (terminals); data acceptance and transfer towards equipment at the control points and other defined or random locations inside the area of remit of the Port of Šibenik. Basic records are "ingress/egress" and "check" (Control records), and
4. *Backup system;* used to ensure business continuity in case of unforeseen and undesirable events.

Functionality of the system within the identified scope will be ensured by development and tight integration of the three distinctive modules:

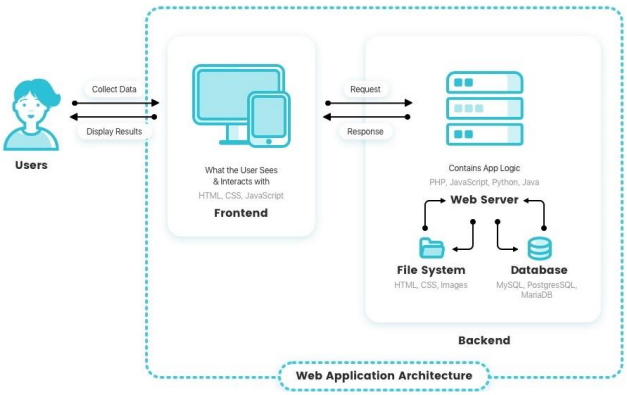

Figure 2: Basic application architecture

1. *PC application* - A stationary register and back-end reporting and oversight component. Central PC application is used to sell all products envisaged as a part of the project, fulfil all requirements of all user categories and pay for the product and activate or deactivate them. For those user categories that need permanent ID cards, there is an option to issue RFID cards.
2. *Police (Ministry of Internal Affairs) PC application design* - a derivative of the base PC application that has a single basic function which is the overview and processing of the created requests for access to the port area. Police employee or a security designated person can deny access without changing the requests. Comments can be entered. Basic reporting functions will be envisaged to view requests that have been cancelled ex post – in order to check the work of the police and security officers. Police officer is a dedicated class of the user representing himself using ID badge number.
3. *Portable Android application* - Serves as a terminal that can be used to read the QR code from the ID pass or printer paper or enter the data contained in the ID pass (for example, vehicle registration plate) in order to check the status. Checks are entered in the system along with supplemental data related to location, time, means of control and control end results.

For each of the four described modules, functions, description, end results and a minimum dataset will be developed, with functional and technical specifications.

V. DISCUSSION

Some useful requirements and suggestions for successful implementation of the ID card and permits issuance have to be identified prior to the commencement of the pilot:

1. *Changes to current Regulation*: They should be relatively minor and primarily include a change in description of the ID cards (colour and composition), and the recognition of virtual ID cards (especially applicable for "daily" category of usage) that are represented by a valid and properly processed database entry.
2. *Technology*: QR codes can be created in a way to contain useful information like location, name and vehicle's license plate. IT system should be robust and follow all modern ICT and cybersecurity requirements. Solution should be in line with GDPR and ensure alignment with national Cybersecurity regulation.
3. *Payment possibilities and end-user* (stakeholder) *satisfaction*: Considering that ID card and permit issuance carries payments for certain categories of private and legal persons and vehicles, integration with payment gateways supporting various means of payment (subscription, credit cards, PayPal, prepaid) would also be highly advisable and trivial for integration, and it would result in high levels of satisfaction for identified stakeholders (end-users).
4. *Integration:* entry and exit gate procedures should be prepared for integration with the future PCS system, in order to use input data. Furthermore, a module for border police will have to be included with entry function enabling police officers in charge to deny entry to a particular terminal.
5. *Other considerations:* Access using mobile or Web application with adequate usability for mobile phones, tablets or other devices with small screens is advised, especially if used by the police, or for field control purposes.

This project involves the introduction of the system that belongs to a group of mission critical components of the Port of Šibenik Authority in the area of the access control. This requires maximum possible system availability by ensuring availability to distributed system parts and application and database collocation (vendor of the system). Energy supply and network links are determined to be critical parts of the required infrastructure. Availability and security of the system needs to be ensured by technical measures and equipment, both on the side of the end user (Port of Šibenik Authority and target groups) and perspective system vendor, divided as follows:

1. *User side:* On the user side, it is required to ensure Internet access in all terminal locations for the QR code reading. As a failover possibility, mobile operator infrastructure and functions of the mobile application will be used.
2. *Vendor side:* Vendor is using external data centre services with constant supervision, uninterruptable dual power supply, and systems for automatic alerting and fire suppression. Cloud backup is used, and it enables periodic data saving to an external server used in high quality data centre. Backup is achieved using replication and network synchronisation, including snapshots that record every change, allowing for data restore from a protected replica, especially in case of disaster. Additionally, data backup is done also using local server. Part of the availability and system security is also end user education, which is envisaged integral part of the system introduction that will be also completed as an integral part of the end package delivery and development.
3. *Used technologies:*

a. *Web application* development will use the following technologies: ASP.net, JavaScript, Ajax, Bootstrap,

b. *PC application* development will use Visual Studio c#, and

c. *Mobile application* development will use the following technologies: Android studio, Java.

Direct added value of the project is the further extension of the gathered and processed information towards end users - passengers, thus enabling direct benefits. For example, a QR code, or similar interconnectivity technology may be used as a form of notification that would be posted at the passenger terminal, or using digital outlets with similar functionality, which would allow passengers to download and install a mobile application to their devices, and access visual representation and data representing all information related to the vessel traffic in the port of Šibenik that is applicable and significant to them.

Financial means required for maintenance of the product are considered to be marginal, and after depreciation and end of functional amortization, it will be replaced within regular asset renewal policy of the Port of Šibenik Authority. The usage of the system will be measured, and this metric will show the utilization by the end users – passengers and stakeholders within the identified target groups. This approach will also provide the metric for further analysis within the DigLogs Transferability Plan [12], which will account for the possibility of transferring the knowledge and the know-how gained through the project implementation.

VI. Conclusion

Access control is a fundamental organizational concept in security with the aim of minimizing risk to the business or organization, in this case a seaport system. It enables the governing authority (the Port Authority) to control access to certain areas of the seaport.

In recent years, the EU has focused on the digitalization and cross-border cooperation as means of closing the technological gap in certain areas and regions. The Port of Šibenik has identified the Interreg DigLogs project as a suitable funding source to close the digital gap posed by lack of a modern streamlined digital business solution for access control. This decision has been greatly impacted by the fact that the development of a national PCS implementation project does not envisage a separate module for access control, rather, it relies on the data exchanged with already existing systems.

Port of Šibenik does not have an automated IT solution for this purpose, and especially not for the passenger traffic segment, hence the motivation for the proposed content of the pilot project. Crucial project components that will be delivered are as a part of the project arethe Web application, PC and mobile application, Police and security application, End user education and training, and Final production work – delivery.

Prior to the application development, data tables, functional and technical specification need to be developed according to the request of the Port of Šibenik Authority and identified processes. Links towards fixed entry and exit points also have to be established in order to facilitate the system functioning.

Final configuration and testing will mark the final phase of the pilot deployment, when the card readers will be connected, all database and production services started, and the system will go live towards identified stakeholders from target groups. Feedback will be gathered and hopefully will be largely positive, in line with stakeholder input received during the previous project activities. Previous experience shows that some received suggestions cannot be acknowledged as a part of the ongoing project, but they will be considered as a part of future system upgrades using other sources.

Possible future venues for extension of this project include knowledge and experience transfer to other ports. For this to happen, it is crucial to develop a transferability plan that will entail past experience and consider the specific requirements of the new implementation project.

Acknowledgement

This work was supported by “DigLogs – Digitalising Logistics Processes” (Interreg V-A Italy – Croatia 2014-2020) project.

References

[1] University of Rijeka, Faculty of Maritime Studies, "2014 - 2020 Interreg V-A Italy - Croatia CBC Programme, Call for proposal 2017 Standard - DigLogs, Priority Axis: Maritime transport Application Form", Rijeka, Croatia, 03.07.2020. (unpublished, internal project documentation)

[2] Port of Šibenik Authority Web Page. [Online]. Available: https://www.portauthority-sibenik.hr [Accessed: 03-Dec-2020]

[3] Aksentijević Forensics and Consulting, Ltd, "Definition of steps to be taken for innovative solutions deployment both from market and policy perspective V2 - Roadmap", DigLogs project, version 0.4 Final, deliverable D4.3.1, Rijeka, Croatia, 30.04.2020. (unpublished, internal project documentation)

[4] M. Jović, “Digital transformation of Croatian seaports,” in 32nd Bled eConference: Humanizing Technology for a Sustainable Society Conference proceedings / Doctoral Consortium, 2019, pp. 1147–1164

[5] E. Tijan, M. Jardas, S. Aksentijević, and A. Perić Hadžić, “Integrating Maritime National Single Window with Port Community System – Case Study Croatia,” in 31ST Bled eConference - Digital Transformation: Meeting the Challenges Conference Proceedings, 2018, pp. 1–11

[6] International Port Community Systems Associations, “How to develop Port Community Systems,” 2015. [Online]. Available: http://www.ipcsa.international/armoury/resources/ipcsa-guideenglish-2015.pdf [Accessed: 01-Dec-2020]

[7] CIMIS - Hrvatski integrirani pomorski informacijski sustav [Online]. Available: https://cimis.pomorstvo.hr [Accessed: 01-Dec-2020]

[8] Port of Šibenik Authority, “Regulation about identification cards of the Port of Šibenik” [Online]. Available: https://www.portauthority-sibenik.hr/dokumenti/pdf/Pravilnik-o-ID-iskaznicama.pdf [Accessed: 01-Dec-2020]

[9] Port of Šibenik Authority, “ID cards price list” [Online]. Available: https://www.portauthority-sibenik.hr/dokumenti/pdf/Cjenik-ID-iskaznica.pdf [Accessed: 01-Dec-2020]

[10] Aksentijević Forensics and Consulting, Ltd, "Pilot project plan - Innovative solution for access control", version 0.3 final version, deliverable D5.2.1, 30.09.2020. internal documentation, Rijeka, Croatia, (unpublished, internal project documentation)

[11] Aksentijević Forensics and Consulting, Ltd, "Access control technical specification", project technical specification, final version, 26.08.2020., Rijeka, Croatia (unpublished, internal project documentation)

[12] Aksentijević Forensics and Consulting, Ltd, "Transferability plan - PP8", version 0.1 Draft, deliverable D5.4.4, 23.11.2020., Rijeka, Croatia, (unpublished, internal project documentation)